Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A validation protocol for a printer consumable ~~determining whether an untrusted authentication chip contained within a consumable is valid, or not,~~ comprising the steps of:

providing a printer containing a trusted authentication chip and a printer consumable containing an untrusted authentication chip;

generating an original random number;

applying, in ~~a~~ the trusted authentication chip~~contained within a consuming device~~, an asymmetric encryption function to the random number using a first key from the trusted authentication chip to produce an encrypted random number;

passing the encrypted random number to the untrusted authentication chip;

decrypting, in the untrusted authentication chip, the encrypted random number with an asymmetric decryption function using a second secret key from the untrusted authentication chip to produce a decrypted random number;

comparing the decrypted random number with the original random number, without knowledge of the second secret key, and in the event of a match considering the printer consumable to be_valid and allowing the consumption of the consumable by the ~~consuming device~~printer; and,

otherwise considering the printer consumable to be invalid and thereby restricting the consumption of the printer consumable by the ~~consuming device~~printer.

2. (Original) A validation protocol according to claim 1, where the random number is not secret, but where the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

3. (Original) A validation protocol according to claim 1, where the first key is a public key.

4. (Original) A validation protocol according to claim 1, where the encryption is implemented in software.

5. (Original) A validation protocol according to claim 1, where the encryption is implemented in a second authentication chip.

6. (Original) A validation protocol according to claim 1, where the keys used for encryption and decryption are 2048 bits or larger.

7. (Currently amended) A validation system for ~~determining whether an untrusted authentication chip is valid, or not,~~ a printer consumable, ~~where~~ the system comprising~~es~~:

a ~~consuming device~~printer containing a trusted authentication chip;

a random number generator to generate an original random number;

an asymmetric encryptor to encrypt the original random number using a first key in the trusted authentication chip;

a printer consumable containing the untrusted authentication chip which receives the encrypted random number, the untrusted authentication chip comprising an asymmetric decryption function to decrypt the encrypted random number using a second secret key for the decryption function to produce a decrypted random number; and

comparison means to compare the decrypted random number with the original random number, without knowledge of the second secret key;

whereby, in the event of a match between the decrypted random number and the original random number, the untrusted chip is considered to be valid, thereby allowing the printer consumable to be consumed by the ~~consuming device~~printer;

otherwise the untrusted chip is considered to be invalid, thereby restricting the printer consumable being consumed by the ~~consuming device~~printer.

8. (Original) A validation system according to claim 7, where the random number generator, encryptor and comparison means are in an external system.

9. (Currently Amended) A validation system according to claim 7, wherein the ~~consuming device is a printer and the~~ consumable device is an ink cartridge.

10. (Original) A validation system according to claim 7, where the random number generator and encryptor are in a second authentication chip, and the comparison means are in an external system which receives the random number and the encrypted version before

passing only the encrypted version to the untrusted chip; the system also receives back the decrypted version from the untrusted chip and performs the comparison.

11. (Cancelled).

12. (Original) A validation system according to claim 7, where the random number is not secret, but the random number generator includes a random function to produce random numbers from a seed, and the function advances after every random number is produced so that the next random number will be produced from a new seed.

13. (Original) A validation system according to claim 7, where the first key is a public key.

14. (Original) A validation system according to claim 7, where the encryption is implemented in software.

15. (Original) A validation system according to claim 7, where the encryption is implemented in a second authentication chip.

16. (Original) A validation system according to claim 7, where the keys used for encryption and decryption are 2048 bits or larger.

17. – 19. (Cancelled).